

FILED

UNITED STATES DISTRICT COURT

JUL 28 2023

for the
Northern District of OklahomaMark C. McCartt, Clerk
U.S. DISTRICT COURTIn the Matter of the Search of
a Black Samsung Cellular Device IMEI:
354519748095909, and a black iPhone with a cracked
back Currently Stored at the DEA Tulsa Resident OfficeCase No. 23MJ-410-MTSFILED UNDER SEAL

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment "A"

located in the Northern District of Oklahoma, there is now concealed (identify the person or describe the property to be seized):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

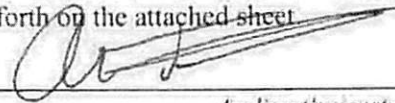
The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. § 846	Drug Conspiracy

The application is based on these facts:

See Affidavit of Special Agent Alan Frank, DEA, attached hereto.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Special Agent Alan Frank, DEA

Printed name and title

Subscribed and sworn to by phone.

Date: 7-28-2023City and state: Tulsa, Oklahoma

Judge's signature

Mark T. Steele, U.S. Magistrate Judge

Printed name and title

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA**

**In the Matter of the Search of
a Black Samsung Cellular Device
IMEI: 354519748095909, and a black
iPhone with a cracked back Currently
Stored at the DEA Tulsa Resident
Office**

Case No. _____

FILED UNDER SEAL

**Affidavit in Support of an Application
Under Rule 41 for a Warrant to Search and Seize**

I, Special Agent Alan Frank, being first duly sworn under oath, depose and state:

Introduction and Agent Background

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C) and am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of officers authorized by the Attorney General to request such a warrant.

3. I am a Special Agent with Drug Enforcement Administration, United States Department of Justice, and as such, I am an investigative or law enforcement officer within the meaning of Title 18, United States Code, Section 2510(7), and Title 21,

United States Code, Section 878(a), that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Titles 18 and 21 of the United States Code. I am a Special Agent with the Drug Enforcement Administration (DEA), United States Department of Justice. I have been a DEA Special Agent since May 2021. I am currently assigned to the Tulsa Resident Office (TRO), in Tulsa, Oklahoma, and I am an “investigative or law enforcement officer” of the United States as defined in Title 21 U.S.C § 878(a). I was previously employed with the St. Louis County Police Department. I worked for St. Louis County Police Department for approximately 6 years, and during that time I was assigned to a Federal Bureau of Investigation (FBI) Violent Gang Safe Streets Task Force as a Special Federal Officer (SFO), where I investigated drug and weapons violation under United States Title 18 and Title 21. I have received numerous hours in specialized training from various federal and local law enforcement agencies. This training has focused upon methods of unlawful manufacturing of illegal narcotics via clandestine laboratories, the installation and monitoring of global positioning satellite (GPS) trackers, Title III wire interceptions, smuggling and distribution techniques, methods of drug trafficking, as well as the means by which drug traffickers derive, launder, and conceal their profits from drug trafficking, the use of assets to facilitate unlawful drug trafficking activity and the law permitting the forfeiture to the United States of assets purchased with drug proceeds or assets used or intended to be used to facilitate the drug violations. I have gained a considerable amount of knowledge about drug trafficking organizations and their

members through my training and experience. During the course of my training and interviews with various defendants I have learned how individuals involved in drug distribution schemes maintain records and conspire to deceive law enforcement as well as rival distributors of controlled dangerous substances. I have learned how individuals who are involved in the distribution of controlled dangerous substances maintain records and secret monies derived from the sale of illegal drugs. I have learned of the distribution schemes utilized by individuals involved in Drug Trafficking Organizations (DTOs).

4. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open-source information including information available on the Internet. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

5. Based on my training, experience, and the facts set forth in this affidavit, there is probable cause to believe that evidence of violations of Title 21, United States Code, Section 846 - Conspiracy to Distribute and Conspiracy to Possess with Intent to Distribute Methamphetamine will be located in the electronically stored

information described in Attachment B and is recorded on the device described in Attachment A.

Identification of the Device to be Examined

6. The property to be searched is a **Black Samsung cellular device IMEI: 354519748095909**, and a **black iPhone with a cracked back**, hereinafter the “Devices.” The Devices are currently located at the DEA Tulsa Resident Office at 7615 East 63rd Place, Suite 250, Tulsa, Oklahoma.

7. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

Probable Cause

8. In approximately January 2022, members of the Drug Enforcement Administration (DEA) Tulsa Resident Office (TRO), United States Postal Inspectors (USPI), and the Tulsa Police Department (TPD), began investigating a drug trafficking organization (DTO) distributing methamphetamine, fentanyl, and cocaine in Tulsa, Oklahoma, and other parts of the United States.

9. From January of 2022, to March of 2022, members of the DTO conducted controlled purchase with the DTO in Tulsa, Oklahoma. The controlled purchases were conducted by an undercover agent (UC). Through the controlled purchases members of the TRO would contact DTO member Jorge Cruz-Diaz in Mexico, and arrange to purchase methamphetamine in Tulsa. In that time period members of the

TRO conducted 4 controlled purchases. Each time, members of the TRO observed a green Toyota Avalon deliver to the UC. Through pre and post surveillance investigators identified the Toyota Avalon would respond from 1202 North Quebec Avenue.

10. On or around March 14, 2022, a traffic stop was conducted on the aforementioned Toyota Avalon. Through the traffic stop investigators identified the driver of the Toyota Avalon to be Carlos Daniel Sanchez-Meza. A photograph of Sanchez-Meza was shown to the UC who identified Sanchez-Meza as the courier responsible for delivering the methamphetamine to the UC during the controlled purchases.

11. On or around May 4, 2022, members of the DEA TRO and USPI executed an anticipatory search warrant authorized by United States Magistrate Judge Susan E. Huntsman. Upon executing the search warrant members of the TRO seized a cellular device belonging to Soledad Perezchica. During a post Miranda interview conducted with Perezchica investigators obtained consent to search Perezchica's cellular device.

12. On or around July 21, 2022, members of the TRO obtained the content of the cellular device. Upon analyzing the data investigators identified multiple Mexico-based Sources of Supply (SOS) responsible for sending methamphetamine and fentanyl to Perezchica. These SOS' were identified to be Samuel Ulises Ortega, FNU LNU a/k/a "Charlie", Agustin Bottello-Valles a/k/a "El 7", and Jose Ortiz-Tapia a/k/a "Pariente".

13. On or about November of 2022, a Tulsa-based DTO member was traffic stopped in Yavapai County Arizona. A probable cause search of the vehicle revealed the DTO member was transporting approximately 53 pounds of methamphetamine, 36 pounds of fentanyl, and 5 kilograms of cocaine. Upon interviewing the DTO member investigators were advised the DTO member was transporting the contraband on behalf of Mexican-based SOS, FNU LNU a/k/a "Charlie".

14. On or February of 2023, members of the TRO conducted an interview with a cooperating defendant (CD-1). During the interview with CD-1, members of the TRO were advised CD-1 began working for the DTO from 2021 to present. CD-1 would drive from Tulsa, Oklahoma to Phoenix, Arizona and obtain large quantities of methamphetamine and fentanyl and traffic the contraband back to Tulsa, Oklahoma. CD-1 advised he/she would drive these loads on behalf of "Charlie" and Ortega. CD-1 advised investigators that one of the locations that CD-1 would deliver the large quantities of contraband to was 1202 North Quebec Avenue, Tulsa, Oklahoma.

15. During the interview with CD-1, CD-1 was shown photographs of DTO members identified by members of the TRO. CD-1 was able to identify multiple members of the DTO and advised their role. One of the DTO members identified by CD-1 was Sanchez-Meza. CD-1 advised when CD-1 would deliver to 1202 North Quebec he/she observed Sanchez-Meza at the residence.

16. On April 5, 2023, Assistant United States Attorney (AUSA) David Nasar and SA Alan Frank presented evidence to the Grand Jury of the Northern District of

Oklahoma (NDOK) which resulted in a True Bill for Carlos Daniel Sanchez-Meza regarding Sanchez-Meza's involvement in a drug conspiracy.

17. On or about July 20, 2023, USPI intercepted a parcel addressed to 825 North Sandusky Avenue, Tulsa, Oklahoma. On that date members of USPI obtained authorization from the Northern District of Oklahoma (NDOK) to open the parcel. USPI advised upon opening the parcel they observed a vacuum sealed bag containing counterfeit M-30 pills. Through training and investigators members of the TRO recognize counterfeit M-30's to be suspected fentanyl pills.

18. On or about July 21, 2023, members of USPI conducted a controlled deliver with the parcel in question. USPI delivered the parcel in question to 825 North Sandusky Avenue. USPI advised a Hispanic male, later identified as Carlos Daniel Sanchez-Meza obtained the parcel in question from the front porch of the 825 North Sandusky, and transported the parcel in question to his vehicle. USPI advised Sanchez-Meza proceed to drive away from the residence at which point Tulsa Police Department (TPD) conducted a traffic stop. USPI advised during the traffic stop they located the parcel in question in the back seat of the vehicle. USPI advised they also located a handgun in the vehicle. USPI stated upon arresting Sanchez-Meza they seized 2 cellular devices. The cellular devices were described as:

- A black Samsung cellular device
- A black iPhone cellular device, the back of the cellular device is cracked

19. USPI advised a record check revealed Sanchez-Meza had an active arrest warrant (see paragraph 16).

20. USPI advised they conducted an interview with Sanchez-Meza. Prior to conducting the interview Sanchez-Meza was read his Miranda warnings to which he advised he understood his rights and wished to speak with investigators.

21. Sanchez-Meza advised he had previously received one other parcel in the mail reference to the DTO in Tulsa. Sanchez-Meza also provided a passcode to the Samsung cellular device.

22. At the conclusion of the interview members of USPI seized the 2 cellular devices as evidence and stored them per USPI policy and procedure.

23. On July 24, 2023, members of the TRO met with USPI regarding the incident on July 21, 2023. At that time members of the TRO obtained custody of the 2 cellular devices in question. Members of the TRO transported the devices to the TRO and stored per DEA policy and procedure.

24. Through this investigation members of the TRO have identified Sanchez-Meza to be a Tulsa-based member of the DTO responsible for distribution, and assisting in coordinating large quantities of contraband to Tulsa.

25. Investigators through training and experience know that it is common for DTO members to utilize their cellular devices to communicate with other DTO members. This communication has been identified to be through conventional wire and electronic communication, however investigators also know that members of the DTO utilize encrypted application such as WhatsApp to communicate DTO business. Investigators know one of the only means to obtain this data is through forensic analysis conducted on seized devices. Through investigators knowledge of

this DTO members of the TRO believe that Sanchez-Meza's seized cellular devices contain content reference to DTO business which would be pertinent in identifying co-conspirators, DTO stash residences in Tulsa, and means to launder drug proceeds.

26. The Devices are currently in storage at 7615 East 63rd Place, Suite 250, Tulsa, Oklahoma, 74133. In my training and experience, I know that the Devices have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the DEA on July 24, 2023.

Technical Terms

27. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving,

and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This

removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.
- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as

wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

- f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.
- g. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP

address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- h. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

28. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

Electronic Storage and Forensic Analysis

29. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have

been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

30. Your affiant knows that cellular telephones are often equipped with digital cameras and those phones possess the capability to transmit and/or store electronic images. Your affiant knows that in many cases, cellular telephones maintain photographs of illegal activities to include evidence of illegal drug trafficking. These photos are sometimes stored in their cellular phones and often are transmitted or sent from one electronic media device to another. Your affiant also knows that cellular phones may also contain notes regarding potential illegal acts that are recorded by the subject who possesses the electronics. Furthermore, your affiant knows that text messages, emails are often used by two or more persons to communicate information regarding illegal activities, between principals and co-conspirators of those crimes.

31. Your affiant knows that cellular telephones are utilized by the majority of individuals in the United States and have become a staple of communication between individuals using text messaging, visual and audible communications (telephone calls and FaceTime type communications) as well as applications like "Whatsapp." Additionally, individuals utilize their cellular devices to take pictures, keep notes, as a GPS (global positioning System) device, and even to conduct illicit or illegal activity. Communications on phones are kept for long periods and transferred from one phone to another when replaced. This is done through the use of Cloud storage and direct transfer conducted at the time of purchase or by the individual themselves. Individuals utilize this method as not to lose data that is

stored on the phone such as contacts, photos, notes, and other important information to the individual. This data includes contacts used to conduct illegal activities to include drug trafficking.

32. Based on my education, training, and experience, I know that individuals involved in the use, sales, manufacturing, and transportation of illegal narcotics often use cell phones and other electronic devices to further their trade by conducting business on them via text messages and phone calls. I also know from my training, education, and experience that:

- a. Drug distributors/traffickers commonly maintain books, records, receipts, notes, ledgers, and other documents/papers both electronically and in paper form, which relate to the transportation, ordering, sale, and distribution of controlled substances, even though such documents may be in code and/or identify customers/sources/co-conspirators through monikers/nicknames. Documentation such as this oftentimes results because drug distributors/traffickers commonly “front” drugs (provide controlled substances on consignment) to their clients and must account for these transactions in order to collect outstanding drug debts.
- b. Drug distributors/traffickers commonly maintain addresses or telephone numbers in notebooks, papers, cellular phones, computers and electronic storage media which reflect names, address, and/or telephone numbers for their associates in the drug distribution/trafficking organization, even if

said items may be in code, and such traffickers send and receive items listed in this affidavit by mail and other common carriers.

- c. Drug users, distributors and traffickers frequently take, or cause to be taken photographs or videotapes of themselves, their associates, their property/assets, and their product, and these individuals usually maintain these photographs or recordings/videos in the residences under their control. These photographs and videos are also often found in the individual's cellular telephone, computers and other electronic storage media.
- d. Cellular telephones are often used to facilitate offenses and allow criminals to maintain communication with each other before, during and after the commission of offenses. I am aware that cellular telephones have the capacity to store a vast amount of information, including but not limited to: telephone numbers, voice messages, text messages, e-mail, photographs, videos, address books, records, phone call histories, contact and other information. This information may be contained on the cellular telephone.
- e. Text messages and e-mails are often used by two or more persons to communicate information regarding illegal activities between two telephones or between one telephone and a personal computer. This information can include directions for deliveries, stash locations, prices, cell phone contact numbers, and instructions.

- f. Cellular telephones often contain stored phone numbers and contact information of individuals that conduct business with other co-conspirators that possess the cellular telephone.
- g. When drug users/dealers/traffickers use text messages to discuss topics such as quantities, prices, and the quality of controlled dangerous substances, as well as dates, times and locations for drug transactions, these communications are often in coded drug talk/jargon and require review by peace officers experienced in deciphering such communications.
- h. In my experience in searching cellular telephones possessed by known drug users/distributors/traffickers, photos and/or videos have been discovered which evidence the use and distribution of controlled dangerous substances and the proceeds intended for or derived therefrom. This evidence often depicts pictures/videos of drugs for showing drug quality, condition or quantity. Moreover, users will commonly document episodes of drug use in social settings. Additionally, drug distributors will take pictures ("trophy" pictures) or otherwise capture digital recordings for the purpose of memorializing their credibility/capability as a drug dealer and accomplishments (acquisition of assets/large amounts of U.S. currency) relating thereto.
- i. In all phases of drug distribution, the utilization of cellular telephones is essential. Drug users/dealers/traffickers use cellular telephones to place calls, as well as communicate by SMS text messaging. As drug dealing

necessarily entails constant communications with accomplices, co-conspirators, clients, and sources, these communications virtually always take place by voice calls and text messaging over cellular telephones.

- j. Cellular telephones are almost always used by drug distributors as a way to communicate. They will communicate by verbal conversations, digital text messaging, and/or sending photographs to one another. To avoid detection, drug distributors will oftentimes speak in coded language or through use of vague messages. Sometimes the cellular telephone numbers they use are listed in a different individual's name or they will frequently change phone numbers. Drug distributors will often "drop" or switch cellular phones to avoid detection by law enforcement. This will result in the accumulation of several different cellular phones.

42. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of use, who used each, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. I know that when an individual uses an electronic device as a communication device or a device to obtain information from the Internet related to a criminal act, the individual’s electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

43. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire

medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

44. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

45. *Methods of examination.* In conducting this examination, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crime(s) under investigation, including but not limited to undertaking a cursory inspection of all information within the Device. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with stored cellular device data, such as pictures and videos, do not store as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications associated with a cellular device, as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications. Consequently, often many

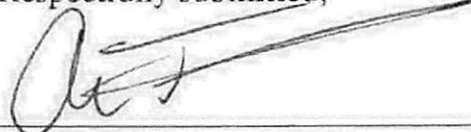
communications in cellular device data that are relevant to an investigation do not contain any searched keywords.

Conclusion

46. Based on the information above, affiant submits that there is probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

47. Affiant requests to be allowed to share this affidavit and the information obtained from this search with any government agency, to include state and local agencies investigating or aiding in the investigation of this case or related matters, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions from this matter.

Respectfully submitted,



Alan Frank
Special Agent
Drug Enforcement Administration

Subscribed and sworn before me on this 28 day of July 2023.



Mark T. Steele
United States Magistrate Judge
Northern District of Oklahoma

ATTACHMENT A

Property to Be Searched

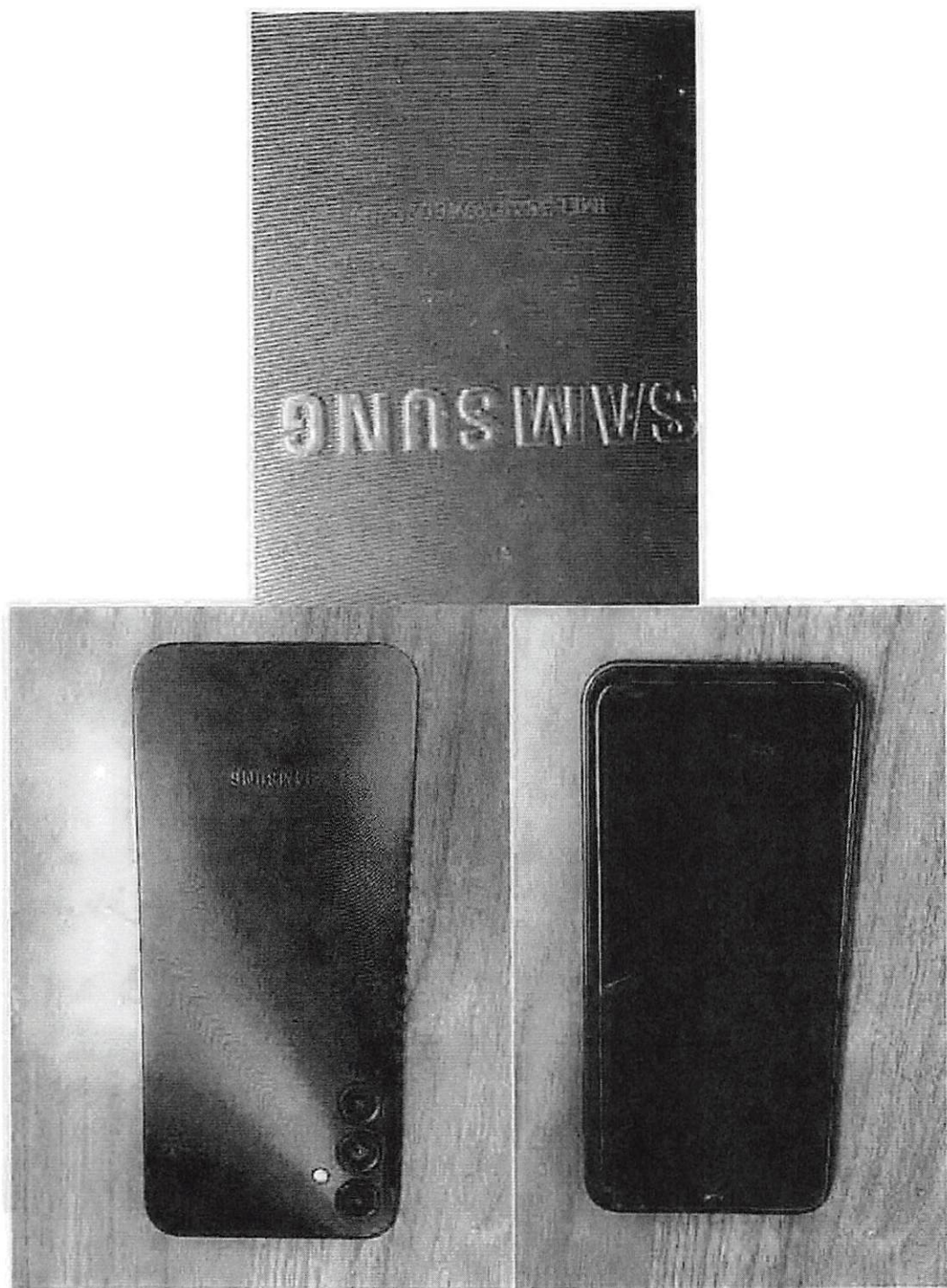
The property to be searched are:

- a Black Samsung Cellular device, IMEI: 354519748095909
- a black iPhone with cracks on the rear of the device

hereinafter the "Devices." The Device(s) is currently located at 7615 East 63rd Place, Suite 250, Tulsa, Oklahoma.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.





ATTACHMENT B

Particular Things to be Seized

All records on the Device(s) described in Attachment A that relate to violations of Title 21, United States Code, Section 846 - Conspiracy to Distribute and Conspiracy to Possess with Intent to Distribute Methamphetamine, including:

1. Records relating to communication with others as to the criminal offense(s) listed above; including incoming and outgoing voice messages; text messages; emails; multimedia messages; applications that serve to allow parties to communicate; all call logs; secondary phone number accounts, including those derived from Skype, Line 2, Google Voice, and other applications that can assign roaming phone numbers; and other Internet-based communication media;
2. Records relating to documentation or memorialization of the criminal offense(s) listed above, including voice memos, photographs, videos, and other audio and video media, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos, including device information, geotagging information, and information about the creation date of the audio and video media;
3. Records relating to the planning and execution of the criminal offense(s) above, including Internet activity, firewall logs, caches, browser history, and cookies, "bookmarked" or "favorite" web pages, search terms that the user

entered into any Internet search engine, records of user-typed web addresses, account information, settings, and saved usage information;

4. Application data relating to the criminal offense(s) above;
5. Lists of customers and related identifying information;
6. Types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
7. Any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information); and
8. All bank records, checks, credit card bills, account information, and other financial records.
9. Evidence of user attribution showing who used or owned the Device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, phone books, saved usernames and passwords, documents, and browsing history;
10. All records and information related to the geolocation of the Device(s) from January 2022 through July 21, 2023;
11. All records and information related to the coordination, agreement, collaboration, and concerted effort of and with others to violate the criminal statutes listed above.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.